Jurnal Nasional Komputasi dan Teknologi Informasi
Vol. 4 No. 1, Februari 2021
P-ISSN 2620-8342
E-ISSN 2621-3052

Enkripsi Database Sekolah SMK Pembangunan Dengan Algoritma IDEA

Devlin Iskandar Saragih[1*], Paska Marto Hasugian[2]
[1,2]STMIK Pelita Nusantara
Jl. Iskandar Muda No. 1 Medan 20154 Indonesia
Corresponding author's e-mail: 1devlin.iskandar16@gmail.com

Abstrak—Salah satu algoritma didalam kriptografi yang dapat digunakan untuk keamanan database sekolah adalah algoritma IDEA (International Data Encryption Algorithm). Algoritma IDEA merupakan salah satu algoritma kriptografi yang mempunyai berbagai pengaplikasian dalam pengiriman data yang aman pada lingkup jaringan dan sistem pengukuran terdistribusi. Hasil Enkripsi tampil dalam bentuk notepad. Tombol Open data digunakan untuk mencari data yang akan digunakan untuk dilakukan proses enkripsi. Ceklis kunci digunakan untuk menginput panjangnya kunci yang akan digunakan untuk proses pengamanan enkripsi dekripsi. Sistem menampilkan kunci Kriptografi IDEA, dapat menggunakan kunci Kriptografi IDEA, proses perubahan enkripsi dan dekripsi tampak jelas. Enkripsi dilakukan pada database Sekolah SMK Pembangunan dengan algoritma IDEA dan merancang aplikasi enkripsi Database siswa berdasarkan nama Sekolah SMK Pembangunan menggunakan Bahasa pemrograman Visual Basic.
Kata kunci: database, enkripsi, Kriptografi, algoritma IDEA

Abstract—One of the algorithms in cryptography that can be used for school database security is the IDEA (International Data Encryption Algorithm) algorithm. The IDEA algorithm is one of the cryptographic algorithms that has various applications in secure data transmission in the scope of networks and distributed measurement systems. Encryption results appear in the form of a notepad. The Open data button is used to find data that will be used for the encryption process. The key checklist is used to input the key length that will be used for the encryption decryption security process. The system displays the IDEA Cryptographic key, can use the IDEA Cryptographic key, the encryption and decryption change process is clearly visible. Encryption is done on the SMK Pembangunan school database with IDEA algorithm and designing the student database encryption application based on the name of the SMK Pembangunan using Visual Basic programming language.
Keywords: database, encryption, cryptography, IDEA algorithm

1. Pendahuluan

Masalah keamanan data dan informasi merupakan salah satu aspek penting dari sebuah sistem informasi komputer[1]. Salah satu contoh masalah keamanan data yaitu keamanan database di sekolah. Database sekolah merupakan kumpulan data penting bagi sekolah itu sendiri. Didalam database itulah semua data tersimpan. Data yang tersimpan mencakup adalah data sekolah, data pelajar, data guru, data penggajian dan data inventaris sekolah. Permasalahan yang terjadi pada database sekolah yaitu masalah pencurian data dan informasi. Untuk itu dilakukanlah teknik enkripsi pada database sekolah agar isinya tidak dapat dicuri, dibaca, dimanipulasi, dan dibocorkan oleh orang yang tidak bertanggung jawab. Teknik enkripsi membuat isi dari database berubah menjadi kode-kode tertentu yang tidak dapat dibaca isinya [2].

Algoritma IDEA digunakan karena memberikan keamanan tingkat tinggi berdasarkan kunci rahasia yang kompleks, dapat diimplementasikan secara lebih ekonomis dan efisien dalam komponen elektronik serta dilindungi dengan paten untuk mencegah penipuan dan pembajakan algoritma tersebut. Fungsi keberadaan kriptografi IDEA diperlukan sebagai cara untuk mengamankan isi dari database sekolah SMK Pembangunan agar aman dari pencurian data. Penelitian sebelumnya yang membahas tentang Kriptografi IDEA seperti, penelitian berjudul Metode Enkripsi Dan Deskripsi Data Menggunakan Kriptografi IDEA menyatakan bahwa Hasil kriptografi dengan menggunakan metode kriptografi IDEA menghasilkan *chipertext* dengan karakteristik tertentu [3]. *Chipertext* yang dihasilkan berbeda-beda untuk setiap plaintext dan kuncinya. Ini sangat efektif jika digunakan untuk pengamanan suatu data atau password. Karena untuk proses enkripsinya user memerlukan *Plain Text* dan Kunci. Jika salah satu variabelnya berbeda maka hasil chippertextnya sudah tentu berbeda. Penelitian berjudul Perancangan Aplikasi Kriptografi dengan Metode IDEA menyatakan bahwa Aplikasi dapat menginformasikan hasil proses pembentukan kunci, enkripsi dan dekripsi dan hasil proses pada perangkat lunak [4]. Penelitian Implementasi metode kriptografi international data *encryption algorithm* (idea) untuk pengamanan data berita publik khatulistiwa televisi Bontang menjelaskan sebuah aplikasi kriptografi

Copyright © Jurnal Nasional Komputasi dan Teknologi Informasi (JNKTI)

yang dapat mengamankan data berita dengan mengubah isi pesan yang ada dalam data berita. Menggunakan metode *kriptografi International Data Encryption Algorithm* (IDEA) yang merupakan kriptografi simetris dengan memanfaatkan penggunaan satu kunci saja untuk banyak data dalam proses enkripsi dan dekripsi [5]. Hasil dari pembangunan aplikasi kriptografi data berita pada Publik Khatulistiwa Televisi Bontang diharapkan dapat mengurangi tingkat pencurian dan duplikasi data, serta meningkatkan keamanan data berita dalam internal Publik Khatulistiwa Televisi Bontang maupun eksternal dengan rekan media yang lain [6].

2. Tinjauan Pustaka

2.1. Kriptografi IDEA

Kriptografi adalah kata yang berasal dari bahasa Yunani yakni kriptos yang artinya tersembunyi dan graphia yang artinya sesuatu yang tertulis, sehingga kriptografi dapat disebut sebagai sesuatu yang tertulis secara rahasia [7]. Kriptografi merupakan suatu bidang ilmu yang mempelajari tentang bagaimana merahasiakan suatu informasi penting ke dalam suatu bentuk yang tidak dapat dibaca oleh siapapun serta mengembalikannya kembali menjadi informasi semula dengan menggunakan berbagai macam teknik yang telah ada sehingga informasi tersebut tidak dapat diketahui oleh pihak manapun yang bukan pemilik atau yang tidak berkepentingan [8].

IDEA merupakan algoritma simetris yang beroperasi pada sebuah blok pesan terbuka dengan lebar 64 bit dan panjang kunci berukuran 128 bit. IDEA merupakan *block cipher* (cipher blok), yang beroperasi pada blok plaintext 64 bit [9]. Panjang kuncinya 128 bit. Algoritma yang sama digunakan untuk proses enkripsi dan dekripsi. Sebagaimana algoritma enkripsi yang lain, IDEA menggunakan *confusion* dan *diffusion*, berbeda dengan DES yang menggunakan permutasi dan substitusi untuk confusion dan diffusion, IDEA menggunakan operasi aljabar yang tidak kompatibel sebagai berikut :

a. XOR.
b. Penambahan modulo 216.
c. Perkalian modulo 216+1 (operasi ini menggantikan kotak-S atau S-Box).

2.2. Algoritma IDEA (International Data Encryption Algorithm)

Algoritma IDEA (International Data Encryption Algorithm) menggunakan perkalian modulo 216+1. Perkalian dengan nol selalu menghasilkan nol dan tidak memiliki inversi. Perkalian modulo n juga tidak memiliki inversi jika angka yang dikalikan tidak relatif prima terhadap n. Sementara algoritma kriptografi memerlukan operasi yang memiliki inversi. Angka 65537 (216+1) adalah sebuah bilangan prima. Oleh karena itu, operasi perkalian modulo (216+1) pada algoritma IDEA memiliki inversi.

Jika kita membentuk suatu tabel perkalian untuk bilangan-bilangan mulai dari 1 sampai 65536, maka setiap baris dan kolom hanya berisi setiap bilangan satu kali saja. Dalam Algoritma IDEA untuk operasi perkalian, bilangan 16 bit yang terdiri dari nol semua dianggap sebagai bilangan 65536, sedangkan bilangan lainnya tetap sesuai dengan bilangan tak bertanda yang diwakilinya. Algoritma IDEA ini dapat dibagi menjadi dua bagian besar, yaitu enkripsi dan dekripsi [10]. Kriptografi atau metode IDEA (International Data Encryption Algorithm) dimaksudkan sebagai pengganti DES (Data Encryption Standard). IDEA adalah revisi minor cipher yang lebih awal, yakni PES, dan pada awalnya disebut IPES (Improved PES). IDEA didesain di bawah kontrak Hasler Foundation [11].

Algoritma utama dari sistem kriptografi IDEA adalah sebagai berikut :

1. Proses enkripsi : ek (M) = C
2. Proses dekripsi : dk (C) = M

e = adalah fungsi enkripsi ; d = adalah fungsi dekripsi ; M = adalah pesan terbuka (plainteks) ; C = adalah pesan rahasia (cipherteks) ; K = adalah kunci enkripsi atau dekripsi.

3. Metode Penelitian

Setelah melakukan analisis data dengan menggunakan data input yang dibuat, maka dilakukan proses enkripsi dan dekripsi berdasarkan input masukan yang dilakukan. Tujuannya adalah untuk mengetahui proses jalannya algoritma *IDEA* dan untuk membangun keamanan dalam system database Sekolah SMK Pembangunan. Sistem ini akan menghasilkan output berupa informasi hasil enkripsi dekrisi dari algoritma *IDEA*.

Arsitektur prosesor Kriptografi IDEA :

1. Blok Penyandi IDEA

Blok ini berfungsi untuk melakukan proses penyandian data. Jika sub- kunci yang diproses oleh blok ini berupa sub-kunci enkripsi maka pesan yang dihasilkan adalah pesan rahasia (Chipertext) dan jika yang diproses berupa

Copyright © Jurnal Nasional Komputasi dan Teknologi Informasi (JNKTI)

sub-kunci deskripsi maka pesan yang dihasilkan adalah pesan sebenarnya (Plaintext).

2. Blok pembangkit sub-kunci

Blok ini berfungsi untuk membentuk 52 buah sub-kunci enkripsi 16 bit dari kunci enkripsi 128 bit. Sehingga membentuk 52 buah sub-kunci dekripsi 16 bit dari kunci dekripsi 128 bit.

3. Blok port data-in

Blok ini berfungsi untuk membaca 2 buah blok data masukan 32 bit dan penyimpanannya sebagai blok data masukan 64 bit yang akan dienkripsi atau didekripsi.

4. Blok port data-out

Blok ini berfungsi untuk mengeluarkan blok data keluaran 64 bit yang merupakan hasil enkripsi atau dekripsi dengan cara membagi menjadi 2 buah blok data keluaran 32 bit.

5. Blok port kunci-n

Blok ini berfungsi untuk membaca 4 buah blok kunci 32 bit dan menyimpannya sebagai blok kunci 128 bit.

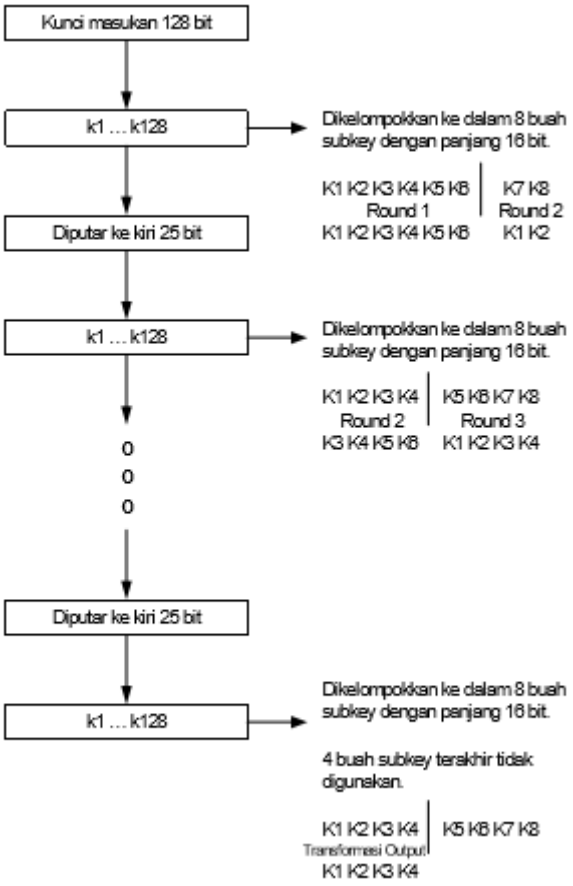
6. Blok mode operasi

Blok ini berfungsi untuk menentukan mode operasi yang digunakan pada proses enkripsi dan dekripsi.

7. Blok control

Blok ini berfungsi untuk mengontrol operasi antara blok fungsional yang menyusun sebuah blok besar seperti sinkronisasi transfer data antara blok.

Perhitungan Algoritma IDEA dalam penyandian data mengamankan data dengan proses enkripsi dan dekripsi.



Gambar 1. Tahapan Algoritma IDEA

4. Hasil dan Pembahasan

Perhitungan Manual Kriptografi *IDEA* Pada Perhitungan Ini Menggunakan Sampel Ukuran Normal 16 Karakter yang diambil dari salah satu nama siswa/i Sekolah SMK Pembangunan Pada Key Input:

Copyright © Jurnal Nasional Komputasi dan Teknologi Informasi (JNKTI)

Algoritma *IDEA* memiliki input-an 128 bit key yang identik dengan 32 digit heksadesimal ataupun 16 karakter untuk menghasilkan 52 subkey. Adapun proses pembangkitan kunci pada algoritma *IDEA* adalah sebagai berikut: Input Plainteks : EVI ARIAN IDAMANIK

Key : IDAMANIK (sebagai sampel menggunakan 8 huruf dibelakang nama plaienteks untuk digunakan sebagai kunci). Hasil dari konversi ke biner dipecah menjadi masing masing 8 kelompok angka, misalnya nomor 1 dan nomor 2 digabung menjadi 1 putaran, lalu nomor 3 dan 4 juga menjadi 1 putaran begitu juga seterusnya. Dibawah ini merupakan tabel 4.3 yang berasal dari gabungan konversi biner. Selanjutnya gabungan dari kunci tersebut disejajarkan atau dipanjangkan untuk selanjutnya dilakukan putaran ke sebelah kiri sebanyak 25 karakter.

Putaran ke 2: Left shift sebanyak 25 karakter:

(01000101010101100100100101000001010100100100100101000001010011100100100101000100000010100110101000001010011100100100101001011)

Menjadi:

1000001010100100
1001001010000010
1001110010010010
1000100010000010
1001101010000010
1001110010010010
1001011010001010
1010110010010010

Hasil dari konversi ke biner dipecah menjadi masing masing 8 kelompok angka, misalnya nomor 1 dan nomor 2 digabung menjadi 1 putaran, lalu nomor 3 dan 4 juga menjadi 1 putaran begitu juga seterusnya. Dibawah ini merupakan tabel 4.3 yang berasal dari gabungan konversi biner. Langkah tersebut dilakukan sampai 8 putaran berjumlah 7 kali.

Selanjutnya gabungan dari kunci tersebut disejajarkan atau dipanjangkan untuk selanjutnya dilakukan putaran ke sebelah kiri sebanyak 25 karakter. Langkah ini dilakukan sampai putaran ke 7.

Tabel 1. Konversi Gabungan Kunci

No	Gabungan Kunci	Simbol
1.	01010000 01010100	X1
2.	10010010 01010000	X2
3.	01010011 10010010	X3
4.	01010001 00010000	X4

Enkripsi dipakai untuk menyandikan suatu data atau informasi. Namun Berdasarkan cara dalam memproses plaintext cipher dapat digolongkan menjadi dua jenis cipher yaitu Stream chiper untuk memproses masukan dan menghasilkan suatu data pada saat bersamaan dan blok chiper yang berkerja dengan memproses suatu data secara blok, dengan menggabungkan beberapa karakter menjadi satu blok. Pada proses enkripsi ini kita menggunakan cipher blok. Proses Meng-enkripsi algotima *IDEA* dapat dilakukan sebagai berikut, Langkah awal ,plaintext 64 bit akan dibagi atau dipecah menjadi 4 buah subblok, masing-masing subblok panjangnya 16 bit, yaitu X1, X2, X3, X4. Keempat subblok tersebut menjadi masukan bagi setiap iterasi tahap pertama pada algoritma *IDEA* dan dengan total 8 iterasi. Lalu subblok yang 16 bit ditransformasikan menjadi sebuah subblok 16 bit dimana subblok yang ditransformasikan tersebut menjadi pesan rahasia 64 bit. Adapun subblok yang ditransformasikan kedalam 16 bit yaitu Y1, Y2, Y3, Y4. Setiap iterasi, keempat subblok tersebut di XOR kan, dengan menggunakan 6 buah subkey yang panjangnya 16 bit. Pertukarkan sub blok yang kedua dan ketiga. kemudian 4 buah dari sub blok dikombinasi dengan 4 subkey didalam transformasi output nya. Tahapannya adalah sebagai berikut:

1. Kalikan blok X1 dengan K1 mod $(2^{16} + 1)$.
2. Tambahkan blok X2 dengan K2 mod $2^{16.}$
3. Tambahkan blok X3 dengan K3 mod $2^{16.}$
4. Kalikan blok X4 dengan K4 mod $(2^{16} + 1)$.

Copyright © Jurnal Nasional Komputasi dan Teknologi Informasi (JNKTI)

5. XOR kan hasil dari step 1 dan 3.
6. XOR kan hasil dari step 2 dan 4.
7. Hasil dari step 5 dikalikan dengan K5 mod (2^{16} + 1).
8. Hasil dari step 6 ditambahkan dengan step 7 mod 2^{16}.
9. Kemudian step 8 dikalikan dengan K6 mod (2^{16} + 1).
10. Kemudian hasil dari step 7 Tambahkan dengan Step 9.
11. XOR kan hasil dari step 1 dan 9.
12. XOR kan hasil dari step 3 dan 9.
13. XOR kan hasil dari step 2 dan 10.
14. XOR kan hasil dari step 4 dan 10.

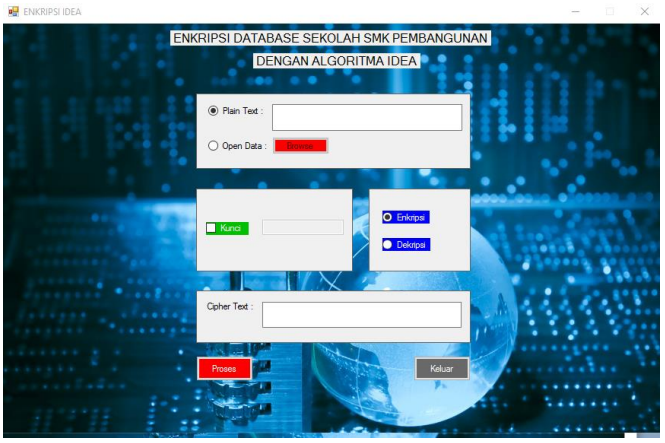
Output dari setiap round adalah empat sub blok yang dihasilkan pada langkah 11, 12, 13 dan 14. Sub blok 12 dan 13 di-swap (kecuali untuk putaran terakhir) sehingga input dari putaran berikutnya adalah hasil kombinasi dari langkah 11 13 12 14.Setelah 8 putaran, akan dilakukan tranformasi output berikut, 1. Kalikan X1 dengan subkey K1 mod (2^{16} + 1).
2. Tambahkan X2 dengan subkey K2 mod 2^{16}.
3. Tambahkan X3 dengan subkey K3 mod 2^{16}.
4. Kalikan X4 dengan subkey K4 mod (2^{16} + 1).

Langkah-langkah Proses Enkripsi:
Plainteks : EVIARIANIDAMANIK Key : IDAMANIK
Proses Enkripsi : sampai pada putaran 7 hanya 4 pecahan kunci terakhir yang digunakan, sehingga menjadi :
Ke 1 (Transformasi Output) = 01011000 = X1
Ke 2 (Transformasi Output) = 10000110 = X2
Ke 3 (Transformasi Output) = 11001010 = X3
Ke 4 (Transformasi Output) = 01011101 = X4
Hasil Proses Binary dalam tabel 2.

Tabel 2. Putaran 7 Hasil Dekripsi

NO	Simbol	Biner	Heksa
1.	X1	01011000	58
2.	X2	10000110	86
3.	X3	11001010	ca
4.	X4	01011101	5d

Setelah masuk ke menu login, maka akan tampil menuju menu pengenalan judul “Selamat Datang Enkripsi Database Sekolah SMK Pembangunan Dengan Algoritma IDEA” dengan logo Sekolah dan Kampus STMIK Pelita Nusantara. Klik tombol warna merah untuk menuju menu Perhitungan.



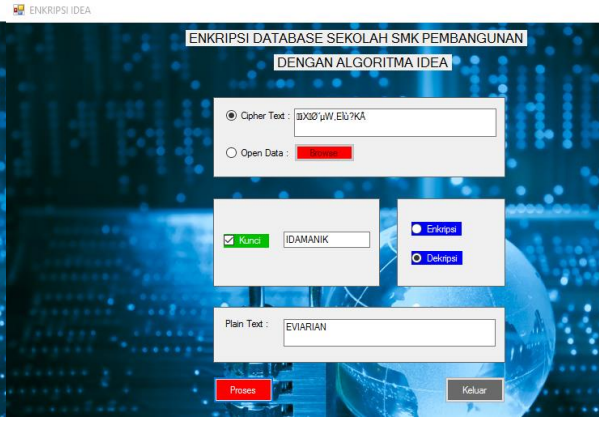
Copyright © Jurnal Nasional Komputasi dan Teknologi Informasi (JNKTI)

Gambar 2. Tampilan Perhitungan Enkripsi

Pada menu perhitungan enkripsi terdapat 2 tombol radio button yaitu Plain

Text dan Open Data, Tombol Ceklis kunci, radio button enkripsi dan dekripsi, Ciphertext, Tombol Proses dan tombol keluar. Tombol plain text digunakan untuk menginput kata yang akan digunakan untuk dienkripsi.Tombol Open data digunakan untuk mencari data yang akan digunakan untuk dilakukan proses enkripsi. Ceklis kunci digunakan untuk menginput panjangnya kunci yang akan digunakan untuk proses pengamanan enkripsi dekripsi. Panjang Kunci harus 8 digit. Radio button enkripsi untuk mengubah tulisan atau kata menjadi berubah, sedangkan radio button dekripsi untuk mengembalikan tulisan atau kata menjadi semula. Tombol Proses digunakan untuk melakukan proses enkripsi dan dekripsi. Tombol keluar digunakan untuk keluar dari aplikasi.

Gambar 3. Penggunaan Plain Text Dan Hasil Cipher Text



Gambar 4. Penggunaan Plain Text Dan Hasil Cipher Text

Gambar 5. Hasil Enkripsi

5. Kesimpulan

Kesimpulan dari penelitian :

1. Kriptografi IDEA memiliki tingkat keamanan yang berlipat dan kuat karena memiliki kunci.
2. Kriptografi dapat melakukan proses enkripsi database sekolah SMK Pembangunan dalam bentuk file excel.

6. Daftar Pustaka

[1] A. Z. F. Rangkuti and H. Fahmi, “Implementasi Kriptografi Untuk Keamanan File Text Dengan Menggunakan Metode MD5,” *J. Nas. Komputasi dan Teknol. Inf.*, vol. 3, no. 2, pp. 170–175, 2020.

[2] A. Ginting, R. R. Isnanto, and I. P. Windasari, “Implementasi Algoritma Kriptografi RSA untuk Enkripsi

Copyright © Jurnal Nasional Komputasi dan Teknologi Informasi (JNKTI)

dan Dekripsi Email," *J. Teknol. dan Sist. Komput.*, vol. 3, no. 2, p. 253, 2015.
[3] R. Kurniawan, P. Studi, I. Komputer, U. Islam, N. Sumatera, and U. Medan, "Rancang Bangun Aplikasi Pengaman Isi File Dokumen Dengan RSA," *J. Ilmu Komput. dan Inform.*, vol. 01, no. November, pp. 46–52, 2017.
[4] N. Laila and A. S. R. Sinaga, "Implementasi Steganografi LSB Dengan Enkripsi Vigenere Cipher Pada Citra," *Sci. Comput. Sci. Informatics J.*, vol. 1, no. 2, p. 47, 2019.
[5] D. Laoli, B. Sinaga, and A. Sindar, "Penerapan Algoritma Hill Cipher Dan Least Significant Bit (LSB) Untuk Pengamanan Pesan Pada Citra Digital," *JISka*, vol. 4, no. 3, pp. 1–11, 2020.
[6] H. Nasution, "untuk Enkripsi dan Dekripsi Query Database pada Aplikasi Online Test (Studi Kasus : SMK Immanuel Pontianak)," vol. 5, no. 1, pp. 1–5, 2017.
[7] Novelius Buulolo and A. Sindar, "Analisis dan Perancangan Keamanan Data Teks Menggunakan Algoritma Kriptografi DES (Data Encryption Standard)," *J. Ilm. Teknol. Inf.*, vol. XV, no. November, pp. 61–65, 2020.
[8] G. A. Nuryanto *et al.*, "Implementasi Kriptografi Pada Aplikasi Memo Berbasis Android," pp. 978–979, 2019.
[9] L. Penjualan and H. Berbasis, "IMPLEMENTASI METODE KRIPTOGRAFI IDEA pada PRIORITY DEALER untuk LAYANAN PEMESANAN dan LAPORAN PENJUALAN HAMDPHONE BERBASIS WEB," *IMPLEMENTASI Metod. KRIPTOGRAFI IDEA pada Prior. Deal. untuk LAYANAN PEMESANAN dan Lap. PENJUALAN HAMDPHONE Berbas. WEB*, pp. 1–7.
[10] Rosmasari, R. A. D. RA, N. Dengen, and M. Taruk, "Implementasi Metode Kriptografi International Data Encryption Algorithm (IDEA) Untuk Pengamanan Data Berita Publik Khatulistiwa Televisi Bontang," *J. Rekayasa Teknol. Inf.*, vol. 2, no. 2, pp. 172–181, 2018.
[11] M. A. Wijaya, W. Kurniawan, and A. Kusyanti, "Perancangan dan Implementasi Algoritma Enkripsi Idea pada Perangkat Kriptografi Berbasis FPGA," *J. Pengemb. Teknol. Inf. dan Ilmu Komput. Univ. Brawijaya*, vol. 2, no. 12, pp. 6973–6981, 2018.

Copyright © Jurnal Nasional Komputasi dan Teknologi Informasi (JNKTI)